Intro
When you set up Windows, we ask that you choose settings relating to your privacy. **You can update your settings any time by going to Start > Settings**.

The information below explains what data we collect and how it is used, depending on the settings you choose. Please be sure to review the full Microsoft Privacy Statement for more information on the personal data we collect and how it is used when you use Windows (type ***aka.ms/privacy*** into any browser window to do so). The data we collect is sent to and stored in the USA and other countries as set forth in the Microsoft Privacy Statement.

Location
The device location setting enables certain Windows features such as auto-setting the time zone or Find my device to function properly. When the device location setting is enabled, the Microsoft location service will use a combination of global positioning service (GPS), nearby wireless access points, cell towers, and your IP address to determine your device’s location. Depending on the capabilities of your device, your device’s location can be determined with varying degrees of accuracy and may in some cases be determined precisely.

If you have enabled the device location setting, your device sends de-identified location information (including wireless access point information, cellular tower information, and precise GPS location if available) to Microsoft after removing all personally identifiable information at the device. This de-identified copy of location information is used to improve Microsoft's location services and, in some instances, shared with our location service provider partners, currently HERE (see https://www.here.com/), to improve the location services of the provider.

Additionally, with this setting enabled you allow apps to use your device’s location and location history to deliver location-aware services. When your location is used by a location-aware app or Windows service or feature, your location information and recent location history are stored on your device. Once your device completes the setup process you will also be able to grant specific apps access to your device’s precise location depending on the capabilities of your device. Otherwise the location information provided to the app has lower accuracy.

If you are signed in with your Microsoft account and location history has been enabled, your last known location information is also saved to the cloud, where it is available across your devices to other apps or services that use your Microsoft account. If you are signed in with your Microsoft account and your device cannot reliably determine your current location on its own (such as when you are in a building or basement), apps or services can use your last known location from your location history that is stored in the cloud if it is available.

There are some exceptions to how your device’s location can be determined that are not directly managed by the location settings.

Desktop apps are a specific type of app that won’t ask for separate permission to discover your device location information and won’t appear in the list that allows

you to choose apps that can use your location. What are desktop apps? They're usually downloaded from the Internet or installed with some type of media (such as a CD, DVD, or USB storage device). They're launched using an .EXE or .DLL file, and they typically run on your device, unlike web-based apps (which run in the cloud).

Even when you've turned off the device location setting, some third-party apps and services could use other technologies (such as Bluetooth, Wi-Fi, cellular modem etc.) to determine your device's location with varying degrees of accuracy. Microsoft requires third-party software developers that develop apps for our Microsoft Store or develop apps using Microsoft tools to respect the Windows location settings unless you've provided any legally required consent to have the third-party developer determine your location. However, to further reduce the risk that an app or service can determine your location when the Windows device location setting is off, you should only install apps and services from trusted sources. For more comprehensive protection of your location, you could consider disabling radio-based components of your device such as Wi-Fi, Bluetooth, cellular modem, and GPS components, which might be used by an app to determine your precise location. However, doing so will also impair other experiences such as calling (including emergency calling), messaging, internet connectivity, and connecting to peripheral devices like your headphones. Please read the privacy policies of the apps and services you've installed to learn more about how they use your device's location.

To facilitate getting help in an emergency, whenever you make an emergency call, Windows will attempt to determine and share your precise location, regardless of your location settings. In addition, your mobile operator will have access to your device's location if your device has a SIM card or is otherwise using a cellular service.

You can turn off the Location setting, control which apps have access to your location and location history, and clear your device's location history at any time by going to **Start** > **Settings** > **Privacy** > **Location**. Learn more about location

Find my device
Find my device uses your device's location data to help you find your device if you lose it. Find my device allows an administrator of a Windows portable device, such as a laptop or tablet, to find the location of that device from account.microsoft.com/devices. To use this feature, the administrator needs to turn on the location setting for the device and sign in to Windows with a Microsoft account. This feature will work for the administrator even if other users have denied access to location for all their apps. When the administrator attempts to locate the device, users will see a notification in the notification area.

You can turn this off at any time by going to **Start** > **Settings** > **Update & security** > **Find my device**. Learn more about Find my device

Online speech recognition

Windows provides both a device-based speech recognition feature (available through the Windows Speech Recognition app) and an online speech recognition service in regions where Cortana is available. To learn what languages and regions speech currently supports, search for “Cortana’s regions and languages” in any browser or in the search bar.

Turning on the Online speech recognition setting lets you use Windows cloud-based speech recognition in Cortana, the Mixed Reality Portal, dictation in Windows from the software keyboard, supported Microsoft Store apps, and over time in other parts of Windows. When you use the Windows online speech recognition service, Microsoft collects and uses your voice recordings to create a text transcription of the spoken words in the voice data. The voice data is used in the aggregate to help improve our online speech services’ abilities to correctly recognize all users’ speech.

You can use device-based speech recognition without sending your voice data to Microsoft. However, the Windows cloud-based speech service provides more powerful recognition than the device-based speech recognition. When the Online speech recognition setting is turned off, speech services that don’t rely on the cloud and only use device-based recognition, like the Narrator app or the Windows Speech Recognition app, will still work, and Microsoft won’t collect any voice data.

You can turn off Online speech recognition at any time in **Start > Settings > Privacy > Speech**. If you later allow Cortana to access information such as calendar and contacts data, your speech recognition experience can be personalized so that it works better for you. Learn more about online speech recognition

Diagnostics
There are two categories of diagnostic data: Required and Optional. Microsoft uses diagnostic data to keep Windows secure and up to date, troubleshoot problems, and make product improvements as described in more detail below. Regardless of your selection, your device will be just as secure and will operate normally. This data is transmitted to Microsoft and stored with one or more unique identifiers that can help us recognize an individual user on an individual device and understand the device's service issues and use patterns.

> **Required** diagnostic data is information about your device, its settings and capabilities, and whether it is performing properly. This is the minimum level of diagnostic data needed to help keep your device reliable, secure, and operating normally.
>
> **Optional** diagnostic data includes information about the websites you browse, how you use apps and features, plus additional information about device health, device activity, and enhanced error reporting. At Optional, Microsoft also collects the memory state of your device when a system or app crash occurs (which may unintentionally include parts of a file you were using when a problem occurred). Required diagnostic data will always be included when you choose to send Optional diagnostic data. While your device will be just as secure and operate normally if you only send Required diagnostic

data, the additional information we collect at Optional makes it easier for us to identify and fix issues and make product improvements that benefit all Windows customers.

Some of the data described above may not be collected from your device even if you choose to send Optional diagnostic data. Microsoft minimizes the volume of data we collect from all devices by collecting some of the Optional diagnostic data from only a small percentage of devices (sample). By running the Diagnostic Data Viewer tool, you can see an icon which indicates whether your device is part of a sample and also which specific data is collected from your device. Instructions for how to download the Diagnostic Data Viewer tool can be found at **Start > Settings >Privacy > Diagnostics & feedback**.

Specific data items collected in Windows diagnostics are subject to change to give Microsoft flexibility to collect the data needed for the purposes described. For example, to ensure Microsoft can troubleshoot the latest performance issue impacting users' computing experience or update a Windows 10 device that is new to the market, Microsoft may need to collect data items that were not collected previously. For a current list of data types collected at both levels of diagnostics, see https://go.microsoft.com/fwlink/?linkid=865126 or see https://go.microsoft.com/fwlink/?linkid=865125 for the current list of data collected at Required.

We use **Required** diagnostic data to keep Windows devices up to date. Microsoft uses:

- Basic error information to help determine whether problems your device is experiencing can be addressed by the update process;
- Information about your device, its settings and capabilities, including applications and drivers installed on your device, to ascertain whether your device is ready for and compatible with the next operating system or app release and ready for update;
- Logging information from the update process itself to understand how well your device's updates are proceeding through the stages of downloading, pre-installation, post-installation, post-reboot, and setup;
- Data about the performance of updates on all Windows devices to assess the success of an update's deployment and to learn device characteristics (e.g., hardware, peripherals, settings, and applications) that are associated with the success or failure of an update; and
- Data about which devices have had upgrade failures and why to determine whether to offer the same upgrade again.

We use both Required and Optional diagnostic data to troubleshoot issues to help keep Windows and related products and services reliable and secure..

Microsoft uses **Required** data to:

- Comprehend the immense number of hardware, system, and software combinations customers use;
- Analyze issues based on specific hardware, system, and software

combinations and identify where problems or issues occur with a specific or limited set of devices;
- Determine whether an app or process experiences a performance issue (e.g., the app crashes or hangs) and when a crash-dump file is created on the device (crash dumps themselves are collected when you choose to send Optional diagnostic data); and
- Understand the effectiveness and fix problems with the diagnostic transmission system itself.

Microsoft uses the additional **Optional diagnostic data** to help spot and fix problems more quickly. We use:
- Information about app activity to understand what the user was doing in an app that caused a problem in conjunction with what we learn about the impact of other apps or processes running on a device;
- Information about device health, such as battery level or how quickly applications respond to input, to better understand the data we collect about application performance issues and make corrections; and
- Information contained in enhanced error reporting and crash dumps to better understand the data related to the specific conditions under which an error or crash occurred.

We use **Required** diagnostic data to improve Windows. We use **Optional** diagnostic data to improve Windows and related products and services.

Microsoft uses **Required** diagnostic data for product improvement in the context of keeping your Windows device up to date and secure; problem-solving; accessibility; reliability; performance; enhancing existing Windows features; compatibility of apps, drivers, and other utilities; privacy; and energy efficiency.

Microsoft uses **Required** data for this purpose as follows:
- Information about customers' devices, peripherals, and settings (and their configurations) is used to prioritize product improvements by determining which improvements will have the greatest positive impact to the most Windows 10 customers; and
- Information about which apps are installed on devices is used to prioritize app-compatibility testing and feature improvements for the most popular apps.

Additional data collected when you choose to send **Optional** diagnostic data is used to help make even more meaningful improvements to Windows and related products and services:
- App activity information helps us prioritize app-compatibility testing and make feature improvements to apps and features that are used the most;
- Information about the impact of device characteristics, configuration, and app activity on device health (for example on battery life) is used to analyze and make changes that improve the performance of Windows devices; and
- Aggregate information about browsing history in Microsoft browsers is used to tune Bing's search algorithms to provide more effective search results.

We don’t use any Windows diagnostic data to provide personalized experiences or promote products or services to you unless you let us do so with the separate **Tailored experiences setting with diagnostic data** (described below).

You can adjust your diagnostic data collection level at any time in **Start** > **Settings** > **Privacy** > **Diagnostics & feedback**. Learn more about diagnostic data

Improve inking and typing
If you choose to send diagnostic data to Microsoft to improve inking and typing recognition, Microsoft will collect samples of the content that you type or write to improve features such as handwriting recognition, autocompletion, next word prediction, and spelling correction in the many languages used by Windows customers. When Microsoft collects inking and typing diagnostic data, it is divided into small samples and processed to remove unique identifiers, sequencing information, and other data (such as email addresses and numeric values) which could be used to reconstruct the original content or associate the input to the user.

You can turn this off at any time in **Start** > **Settings** > **Privacy** > **Diagnostics & feedback**. Learn more about inking and typing data

Tailored experiences with diagnostic data
If you choose to turn on Tailored experiences, we will use your Windows diagnostic data, excluding information about websites you browse, to offer you personalized tips, ads, and recommendations to enhance Microsoft experiences. If you have Required diagnostic data selected as your diagnostic data setting, personalization is based on information about your device, its settings and capabilities, and whether it is performing properly. If you have selected to send Optional diagnostic data, personalization is also based on how you use apps and features, plus additional information about the health of your device. We do not use information about websites you browse, content of crash dumps, speech, typing, or inking input data for personalization when we receive such data from users who have selected to send Optional diagnostic data.

Tailored experiences include suggestions on how to customize and optimize Windows, as well as ads and recommendations for Microsoft and third-party products and services, features, apps, and hardware for your Windows experiences. For example, to help you get the most out of your device, we may tell you about features you may not know about or that are new. If you are having a problem with your Windows device, you may be offered a solution. You may be offered a chance to customize your lock screen with pictures, or to be shown more pictures of the kind you like, or fewer of the ones you don’t. If you stream movies in your browser, you may be recommended an app from the Microsoft Store that streams more efficiently. Or, if you are running out of space on your hard drive, Windows may recommend you try OneDrive or purchase hardware to gain more space.

You can turn this off at any time in **Start** > **Settings** > **Privacy** > **Diagnostics &**

feedback. Learn more about tailored experiences with diagnostic data

Advertising ID
Windows generates a unique advertising ID for each person using a device, which app developers and advertising networks can then use for their own purposes, including providing more relevant advertising in apps. When the advertising ID is enabled, apps can access and use the advertising ID in much the same way that websites can access and use a unique identifier stored in a cookie. Thus, app developers (and the advertising networks they work with) can associate personal data they collect about you with your advertising ID and use that personal data to provide more relevant advertising and other personalized experiences across their apps.

The advertising ID setting applies to Windows apps using the Windows advertising identifier. The advertising ID setting does not apply to other methods of interest-based advertising delivered by Microsoft or third parties, such as cookies used to provide interest-based display ads on websites. Third party products accessed through or installed on Windows may also deliver other forms of interest-based advertising subject to their own privacy policies. Microsoft delivers other forms of interest-based ads in certain Microsoft products, both directly and by partnering with third party ad providers. For more information on Microsoft's other interest-based advertising, click here.

You can turn the advertising ID setting in Windows off at any time in **Start > Settings > Privacy**. Please note that turning advertising ID off will not reduce the number of ads you see, but it may mean that ads are less interesting and relevant to you. Turning it back on will reset the advertising ID. Learn more about advertising ID

Windows Defender SmartScreen
Windows Defender SmartScreen sends data to Microsoft about the websites you visit and files you download to warn you and help protect you and your device from unsafe web content or malicious software. Since we strive to protect you when using our services and those of third parties, we turn Windows Defender SmartScreen on by default.

You can turn Windows Defender SmartScreen off at any time by going to **Start** > **Windows Defender Security Center** > **App & browser control**. Learn more about Windows Defender Smartscreen